STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Computer Security Incident Management

Effective Date: September 1, 2010

Approved: State of Montana Chief Information Officer

I. Statement of Management Commitment

Threats to information systems today include environmental disruptions, human errors, and purposeful attacks by hostile entities such as nation states, terrorist groups, hackers, criminals, and disgruntled employees. Senior management understands their responsibilities in managing the risks from information systems that support the missions and business functions of the organization. Attacks on information systems today are often well organized, disciplined, aggressive, well funded, and in a growing number of documented cases, extremely sophisticated. Successful attacks on public and private sector information systems can result in unauthorized disclosure or modification of highly sensitive information or a mission impacting denial of service.

For risks related to incident management, senior leadership of the organization recognizes that it is essential to make a fundamental commitment to make information security a first-order mission or business requirement.

II. Purpose

This **Computer Security Incident Management Policy** (Policy) establishes the requirements to implement a computer security incident management standard, plan, and associated procedures statewide.

III. Policy Statement

It is the policy of the State of Montana (state) that agencies shall develop and implement an incident management program based on the National Institute of Standards and Technology Computer Incident Handling Guidance and the State of Montana Continuity of Government (COG) plans, policies, standards, and procedures for incident response.

IV. Applicability

This Policy is applicable to agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), which have access, use or manage information assets subject to the policy and standard provisions of §2-17-534, MCA. This Policy shall be communicated to staff and others who have access to or manage information, and information systems and assets.

V. Scope

This Policy encompasses information systems for which agencies have administrative responsibility, including systems managed or hosted by third-parties on behalf of agencies. It addresses security incidents which may occur during normal course of business activities of agencies.

This Policy may conflict with other information system (IS) policies currently in effect. Where conflicts exist, the more restrictive policy governs. The development of future policies or standards will specifically identify and retire any superseded portions of current policies or standards.

VI. Definitions

Agency Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA.

Information Security The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.

Information System A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.

Information Resources Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.

Information Technology Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA.

Refer to the National Institute of Standards and Technology SP800-61 Revision 1 Computer Incident Handling Guide (NIST SP800-61), Appendix D - Glossary for a list of incident management-specific definitions.

Refer to the Statewide Information system Policies and Standards Glossary for a list of local definitions.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information systems security-related definitions.

VII. Authorizations, Roles, and Responsibilities

Refer to the Statewide Guidelines: Information Systems Security, paragraph II Authorizations, Roles, & Responsibilities for applicable authorization, roles, and responsibilities.

VIII. Requirements

This Policy requires that agencies shall:

1. Implement this Policy and its associated standard(s) in compliance to, and integrated with COG plans, policies, standards, and procedure(s) for incident response.

2. Establish a framework to initiate and control the implementation of an incident management program, standard(s) and procedure(s) within agencies, based on standard practices defined by the NIST SP800-61 Computer Security Incident Handling Guide.

IX. Compliance

Compliance with this Policy shall be evidenced by implementation of the Statewide Standard: Computer Security Incident Management and State of Montana Continuity of Government plans, policies, standards, and procedures for incident response.

X. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form (at http://itsd.mt.govcontent/content/policy/policies/action_request.doc). Requests for exceptions are made by submitting an Exception Request form (at http://itsd.mt.gov/content/policy/policies/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

XI. Closing

For questions or comments about this instrument, contact the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

XII. Cross-Reference Guide

A. Federal/State Laws

- §2-15-114 MCA – Security Responsibilities of Departments for Data.

- §2-17-534 MCA - Security Responsibilities of Department.

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- MOM 3-0130 Discipline

C. IT Procedures or Guidelines

- Guide To NIST Information Security Documents
- NIST 800-61 Computer Security Incident Handling Guide
- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

XIII. Administrative Use

Product ID:	POL-20081029a
Proponent:	Chief Information Officer
Version:	1.0.2
Version Date:	2/17/2009
Approved Date:	February 17, 2009
Effective Date:	September 1, 2010
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this architecture paper may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	September 1, 2015
Last Review/Revision:	
Changes:	